Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Personal Data Compliance Under Peru's Law No. 29733 and Supreme Decree No. 016-2024-JUS

Enabling Organizations to Meet Updated Data Protection Requirements

Peru's Law No. 29733, the Personal Data Protection Law, establishes the legal framework for personal data protection in Peru, guaranteeing individuals' fundamental right to control how organizations collect, process, store, and transfer their personal information. The law applies across Peru and extends extraterritorially to any organization, domestic or foreign, that processes personal data belonging to Peruvian residents or uses means located within Peruvian territory. All sectors must comply, including financial services, telecommunications, healthcare, technology, and public administration. Enacted in 2011 and significantly strengthened by Supreme Decree No. 016-2024-JUS, published November 30, 2024, the updated Regulation took effect 120 days after publication, with Data Protection Officer requirements phasing in over one to four years based on company size. Organizations that fail to comply face administrative fines tiered by severity, mandatory corrective measures, and reputational harm from public sanctions listings. Kiteworks enables organizations to meet Law No. 29733 and regulation 016-2024-JUS requirements through secure file sharing, governed data transfers, and comprehensive audit capabilities, which the following paragraphs address in detail. Here's how:

Hardened Virtual Appliance and Encryption for Technical Security Obligations

Articles 9 and 16 of Law No. 29733, extended by Articles 48, 51, and 52 of regulation 016-2024-JUS, require owners of personal data to adopt technical measures that prevent unauthorized alteration, loss, and access, with infrastructure controls aligned to NTP-ISO/IEC 27001:2022. Kiteworks deploys as a single-tenant hardened virtual appliance with a minimized attack surface, automated patch management, intrusion detection, and continuous vulnerability scanning. All personal data at rest is encrypted with AES-256, and organizations may bring their own encryption keys with HSM support to retain full key custody. TLS 1.2 and 1.3 secures every transmission, while automated hash-based integrity verification confirms backup completeness at minimum weekly intervals as Article 51 requires. For electronic transfers leaving organizational infrastructure, Kiteworks enforces authorization controls, applies digital certificates, and performs checksum verification on all outbound files, directly satisfying Article 52's requirements for encrypted transfers with digital signatures and verification checksums.

Solution Highlights

- Hardened single-tenant virtual appliance
- AES-256 encryption with BYOK and HSM support
- Role-based and attribute-based access controls (RBAC and ABAC)
- Data Policy Engine (DPE)
- Automated retention and deletion
- Secure Data Forms
- Immutable audit log
- Real-time SIEM integration

Data Policy Engine and Access Governance for Consent and Data Life-Cycle Requirements

Article 46 of regulation 016-2024-JUS requires organizations to document and implement access life-cycle management with at minimum semi-annual privilege verification, multi-factor authentication mechanisms including digital certificates and hardware tokens, and technical controls preventing unauthorized data reproduction. Articles 28 and 38 of Law No. 29733 require that data banks store personal data in a manner enabling rights fulfillment and delete data automatically when retention periods expire. Kiteworks addresses these obligations through role-based access control (RBAC) and attribute-based access control (ABAC), restricting each user to data their role explicitly authorizes, with automated semi-annual privilege review workflows that produce documented certification results. The Data Policy Engine (DPE) enforces configurable retention schedules by data classification and workspace, automatically flagging and deleting data upon expiry without manual intervention. For sensitive data consent under Articles 13.6 of Law 29733 and 8 of the regulation, Kiteworks Secure Data Forms captures data, storing consent records in strong double encryption with Reference ID and timestamp data.

Compliance Audit Log and SIEM Integration for Incident Documentation and Traceability

Article 46 of regulation 016-2024-JUS mandates that organizations retain traceability records of all logical interactions with personal data for a minimum of two years, available immediately on demand. Article 35 requires that every security incident be documented with full details of facts, effects, and remediation measures to enable verification by the National Authority for Personal Data Protection. Kiteworks generates a tamper-evident compliance audit log capturing every interaction with personal data, including processing, viewing, modification, deletion, import, and export events, each timestamped and attributed to a specific authenticated user with session start and close times. All log records are retained for a configurable period meeting the two-year statutory minimum and export in real time to SIEM platforms including QRadar, LogRhythm, ArcSight, and Splunk. When a security incident occurs, the audit log immediately supplies the documentation package required by Article 34, including affected data categories, approximate data subjects involved, and all remediation actions with timestamps, giving organizations the evidentiary basis to meet the 48-hour notification deadline to the National Authority.

Kiteworks gives organizations operating under Peru's Law No. 29733 and Supreme Decree No. 016-2024-JUS a unified platform to satisfy the regulation's three core compliance domains. Its hardened infrastructure and end-to-end encryption address the technical security obligations that apply to personal data, while built-in access governance tools enforce the consent life-cycle controls and automated data retention policies the regulation demands. When a security incident occurs, the tamper-evident audit log immediately produces the documentation the National Authority for Personal Data Protection requires, and real-time SIEM integration keeps security operations teams equipped to meet the 48-hour notification deadline. Across protection, control, and traceability, Kiteworks translates Peru's updated legal requirements into verifiable, auditable technical controls that organizations can demonstrate to regulators with confidence.